

Cyber JumpStart Portal (FKA MyCyber or Cyber Essentials) Solutions Terms

These Cyber JumpStart Portal – Solutions Terms set forth the terms and conditions of the Modules described herein. The Solution, if purchased by Customer as evidenced by Customer's election on an Order Form, licensed by Customer upon selection/registration within the Cyber JumpStart Portal, or offered by Customer's Authorized Partner and accepted/used by Customer will be provided in accordance with the terms set forth herein and the These Solutions Terms describe the modules (each a "**Module**") that Customer may license and will be provided by Arctic Wolf in accordance with the Cyber JumpStart Portal Subscription Agreement located at <https://arcticwolf.com/terms/cyber-jumpstart-portal-subscription-agreement/> (the "**Agreement**") to which these Solutions Terms are included by reference. Notwithstanding the Platform location which may be set forth on an Order Form, all Security Profile Data stored within the Modules will be stored within Arctic Wolf's third-party service providers' data centers located in the United States. Any capitalized terms not otherwise defined herein shall have the meaning set forth in the Agreement.

Modules:

Cyber Resilience Assessment ("CRA"):

The CRA Module allows Customer to enter and track responses to the various components of industry-standard cyber security frameworks to be offered by Arctic Wolf, in its discretion. Current industry frameworks contemplated within CRA include Controls and Safeguards within the Center for Internet Security ("**CIS**") framework and Profiles and Tiers within the National Institute of Standards and Technology Cybersecurity Framework 1.1 and 2.0 ("**NIST CSF**"). This Module provides a single place to easily create and update responses, track coverage and change of coverage over time, and identify gaps as it relates to the chosen framework.

Eligibility:

- a) Customer or Customer's Users, as defined in the Agreement, and solely for the permitted use set forth therein;
- b) Subscribers who have purchased subscriptions to Arctic Wolf's Managed Detection and Response, Managed Risk, and/or Managed Security Operations Solutions, as defined in the Solutions Agreement located at <https://arcticwolf.com/terms/sa/> (or such other similar executed agreement governing customer's subscription thereof).

JumpStart IR Planner:

The JumpStart IR Planner Module allows Customer to build an effective incident response plan with the key information needed to respond and recover quickly from a cyber incident. This Module provides a single place to easily create and update response team members, external providers, business locations, data center locations, cloud presence information, DNS and hostname data, VDI infrastructure details, response communication plans, endpoint and server monitoring information, and a list of critical business functions, supporting IT systems, and backup information.

Eligibility:

- a) Customers with a subscription to IR Jumpstart Retainer are eligible for this Module.
- b) Eligible customers of Authorized Partners may subscribe to this Module at no cost and subject to the terms of the Agreement

JumpStart Threat Scanner Lite:

The JumpStart Threat Scanner Lite Module permits Customer to scan internet exposed systems for commonly exploited vulnerabilities that are the favorites of cyber attackers. While there are many thousands of possible vulnerabilities, cyber attackers focus on a small number that are easily exploitable. If a system has one of these vulnerabilities, Customer may be at imminent risk for a cyber incident.

Eligibility:

- a) Eligible customers of Arctic Wolf's qualifying insurance carrier and insurance broker partners (excluding any existing Arctic Wolf managed detection and response and/or managed risk customers) may subscribe to this Module at no cost and subject to the terms of the Agreement,
- b) Each such Subscription is subject to the terms of this Agreement and the following usage parameters:
 - i. Maximum number of domain names or IP addresses that can be scanned: 1
 - ii. Automatic scan frequency: No automatic scans are run
 - iii. Automatic email notifications of vulnerabilities found: No automatic emails are sent when vulnerabilities are found
 - iv. Maximum Number of Customer initiated on demand scans allowed per 24 hours: 1

JumpStart Threat Scanner:

The JumpStart Threat Scanner Module permits Customer to scan internet exposed systems for commonly exploited vulnerabilities that are the favorites of cyber attackers. While there are many thousands of possible vulnerabilities, cyber attackers focus on a small number that are easily exploitable. If a system has one of these vulnerabilities, Customer may be at imminent risk for a cyber incident.

Eligibility:

- a) Eligible customers of Arctic Wolf's qualifying insurance carrier and insurance broker partners (excluding any existing Arctic Wolf managed detection and response and/or managed risk customers) may subscribe to this Module.
- b) Each such Subscription is subject to the terms of the Agreement and the following usage parameters:
 - i. Maximum number of domain names or IP addresses that can be scanned: 2048
 - ii. Automatic scan frequency: Scan is run automatically once every 7 days
 - iii. Automatic email notifications of vulnerabilities found
 - iv. Maximum Number of Customer initiated on demand scans allowed per 24 hours: 10

JumpStart Threat Scanner – AWS Marketplace (MP):

This JumpStart Threat Scanner – AWS MP Module permits Customer to scan internet exposed systems for commonly exploited vulnerabilities that are the favorites of cyber attackers. While there are many thousands of possible vulnerabilities, cyber attackers focus on a small number that are easily exploitable. If a system has one of these vulnerabilities, Customer may be at imminent risk for a cyber incident.

Eligibility:

- a) Eligible customers who subscribe to this Module via AWS MP as a twelve (12) month Subscription (beginning on the date of order acceptance on the AWS MP).
- b) Each such Subscription is subject to the terms of the Agreement and the following usage parameters:
 - i. Maximum number of domain names or IP addresses that can be scanned: 10
 - ii. Automatic scan frequency: Scans are not run automatically
 - iii. Automatic email notifications that scan was completed and, if applicable, that a vulnerability(ies) were found
 - iv. Customer may run a total of five (5) scans
 - v. Maximum Number of Customer initiated on demand scans allowed per 24 hours: 10

JumpStart Guides:

The JumpStart Guides Module permits Customer to initiate its cyber risk mitigation journey. Getting started on the journey is difficult because of the overwhelming amount of information, products, and services available. This Module helps Customer get started by focusing on a core set of essential safeguards that significantly reduce risk. Each project includes information about the safeguard and a way for Customer to complete the project by documenting and attesting that Customer has the safeguard in place.

Eligibility:

- a) Customers with a subscription to IR JumpStart Retainer and eligible customers of Authorized Partners may subscribe to this Module at no cost and subject to the terms of the Agreement

Cyber Hygiene Projects:

The Cyber Hygiene Projects Module provides Customer with a collection of tasks and subtasks to guide Customer towards implementing a set of ten security controls that greatly reduce cyber risk. Task management, collaboration, and tracking features allow Customer to interact with others in the progression towards completion. This Module allows Customer to keep tasks and subtasks organized all in one place by assigning tasks to users, making comments, and attaching files and documentation. The ten security controls are Hardening External Exposure, Multi-Factor Authentication, Email Gateway, Backup & Restoration, Endpoint Detection & Response, Privileged Access Management, Network Segmentation, Log Monitoring/Alerting, Inventory & Patch Management, and Security Awareness Training.

Eligibility:

- a) Eligible customers of Arctic Wolf's insurance carrier or insurance broker authorized partners may subscribe to this Module at no cost and subject to the terms of the Agreement

CMMC Readiness:

The CMMC Readiness Module is a collection of tasks and subtasks to guide Customer towards implementing CMMC Level 1, 2 or 3. This Module includes task management, collaboration, and tracking features which allow team members to interact with others in the course of progression towards completion. Eligible customers can use the Module to keep everything organized all in one place by assigning tasks to users, making comments, and attaching files and documentation.

Eligibility:

- a) Eligible customers of Arctic Wolf's insurance carrier or insurance broker authorized partners may subscribe to this Module at no cost and subject to the terms of the Agreement